Peter Alterman, Ph.D.
Senior Advisor for Strategic Initiatives,
Center for Information Technology/National Institutes of Health

# Questions:

1. What trust problems are you trying to solve and for what range of users (e.g. organizations, individuals, health care professionals, consumers)? Please provide some quantitative data if possible to characterize your user base (e.g., percentage or number of each type).

   OpenID/InfoCard: The OpenID Initiative addresses the perceived need for very low assurance electronic identity credentials for use at government websites hosting Level 1 applications. This user base consists of several hundred million accounts worldwide. A more advanced extension of this initiative, which utilizes InfoCard technology, is theoretically capable of providing up to Assurance Level 3 authentication. Like the Level 1 OpenID solution, it relies on the federal e-authentication principle of relying on credentials issued by external parties at known levels of assurance. The user base for InfoCard technology credentials is unknown, but since Microsoft's CardSpace implementation of InfoCard technology ships with all current OS software, the reach is potentially hundreds of millions of users, as well.

   The Collaborative High Assurance Credentialing Initiative (CHACI) is a proposed solution for issuing OMB Level 3 credentials to roughly 85% of the population through a Federal Government / Financial Services industry collaboration. In this model, bank account holders receive Level 3 electronic identity credentials issued by a consortium including vetted Level 3 technology providers and registration/identity proofing by vetted financial services industry partners through one or more routes.

2. Who pays for the solution, implementation, processes and support for your approach? What factors contribute to the total cost of ownership of the technologies, including process costs? What are the implications to widespread deployment?

   OpenID/InfoCard: OpenID credentials are free to end users; costs for deploying and managing OpenID accounts are borne by the credential issuers. InfoCard technology is at a very early stage of implementation and so cost figures have not been developed. Regarding implications of widespread deployment of OpenID (a foregone conclusion), the major consideration is scalability of credential validation, where validation is deemed desirable. InfoCard issues are currently opaque.

   CHACI: After a government seed investment, this initiative proposes that the financial services industry absorb ongoing costs of issuing and managing credentials. Factors that contribute to TCO vary with the several technologies available for implementation. Widespread deployment is built into the design for this approach, since it relies on use of mobile devices, e.g., cellular technology devices, which are used by ~85% of the population. Traditionally underserved segments of the population are disproportionately favored in this model, another benefit.

3. Directory services often support some certificate authority or other authentication mechanism. As you look more broadly at the architecture, how do your approaches work with such directory services?

OpenID/InfoCard and CHACI: NIH is currently deploying a federated Single Sign-On solution that accepts a variety of recognized credential providers using a variety of credential technologies, including OpenID (and InfoCard soon). From a broad architectural perspective, the relationship between federated SSO and directory services is modular, e.g., plug-and-play. Federated trust of external credentials obviates the need to include a directory service. The question of provisioning, attribute/role management and authorization are indeed issues of concern, but these are not strictly directory services.

4. Does your approach support a delegated authentication model where there is an authorized registrar that issues the authentication credentials to individuals? If so, how? Are there implications for interoperability in this scenario?

   Yes, although the terminology of the question is problematic. Both the OpenID / InfoCard initiative and the Collaborative High Assurance Credentialing Initiative are completely compliant with long-standing OMB guidance for leveraging trust in externally-issued electronic identity credentials. Through GSA and the Federal CIO Council, credential providers are vetted against government standards that follow NIST, OMB and CIO Council requirements. Only credentials from successfully vetted providers are trusted by government applications. This model does rely on standing government workgroups and committees but all policies and procedures are mature and have been implemented in practice for a substantial period of time. Interoperability issues are addressed by requirement for vetted credential providers to implement their technologies in compliance with GSA-developed schemes.

5. What should be the role of government? Where can rapid action address common concerns or limitations of trust?

   OMB and the CIO Council have been eloquent and outspoken on the role of government: to reiterate, HSPD-12 requires government agencies to issue high-assurance, cryptographic-based credentials to employees and in-house contractor staff. These credentials should be interoperable within the Federal sphere. Government online applications should rely on electronic identity credentials at appropriate levels of assurance issued by providers whose technology implementations and policies/practices have been successfully vetted by GSA and the CIO Council.

   The desired rapid action would be for the HIT initiative to assert explicitly that authentication solutions must comply with existing Federal electronic identity management policies, practices and methodologies. In this way, current partners will perceive value in their compliance and new partners will have a clear view of requirements and marketplace.